5.4

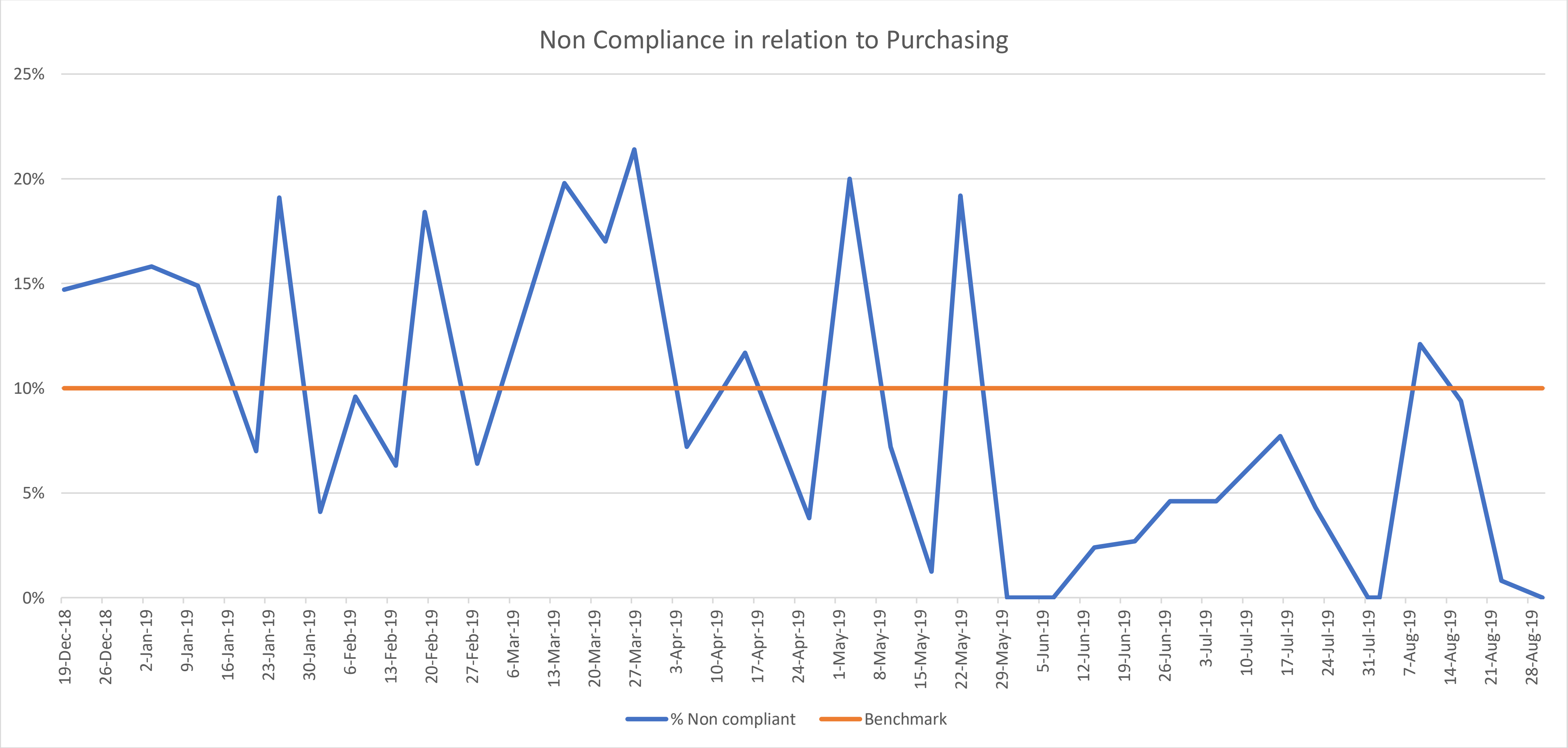
What does fraudulent and corrupt behaviour look like?

Fraudulent and corrupt behaviour can take many forms e.g.

- Misappropriating grant or other funds.
- Taking or requesting inducements to get a particular outcome.
- A manager signing off on fraudulent overtime claims.
- Regularly taking resources, such as office supplies, stationery or other Shire equipment, home for personal use or to sell for personal benefit.
- Unauthorised use of a Shire motor vehicle or credit card.
- Approving invoices for private expenses or colluding to do so for others.
- Submitting a false travel or reimbursement claim and receiving a benefit to which they are not entitled.
- Manipulating recruitment and selection procedures to secure the appointment of a close friend or family member or associate.
- Management promoting, engaging or giving an employee advantage over others for personal reasons.
- Failing to declare a conflict of interest but continuing to deal with a close associate in exercising a Council function (for example, planning or health).
- Accepting or soliciting a bribe or secret commission from a tenderer to give partial consideration to them.
- Providing commercial-in-confidence information to a tenderer resulting in them obtaining an unfair advantage over other tenderers in the tender process.
- Colluding with a supplier of goods or services to the Shire for personal gain.
- Facilitation payments i.e. obtaining kickbacks for organising preferential treatment.
- Gifts or entertainment received which is intended to achieve an outcome in the short or long-term.

5.1

Attachment – Audit (Finance & Risk) Committee – September 2019



5.2

Western Australian
Auditor General's Report

Fraud Prevention in Local Government

Report 5: 2019-20
15 August 2019

5.2

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Gareth Govan
Adam Dias

National Relay Service TTY: 13 36 77
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for those with visual impairment.

ISSN: 2200-1931 (Print)
ISSN: 2200-1921 (Online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

5.2

WESTERN AUSTRALIAN AUDITOR GENERAL’S REPORT

Fraud Prevention in Local Government

Report 5
August 2019

5.2

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

FRAUD PREVENTION IN LOCAL GOVERNMENT

This report has been prepared for submission to Parliament under the provisions of section 25 of the *Auditor General Act 2006*.

This was a narrow scope performance audit, conducted under section 18 of the *Auditor General Act 2006* and in accordance with Australian Auditing and Assurance Standards. Narrow scope performance audits have a tight focus and generally target entity compliance with legislation, public sector policies and accepted good practice.

The audit objective was to assess whether local government entities have taken appropriate steps to prevent fraud.

I wish to acknowledge the cooperation of staff at the local government entities included in this audit.

CAROLINE SPENCER
AUDITOR GENERAL
15 August 2019

Contents

Auditor General's overview

All organisations, public and private, face the risk of fraud. This will remain the case wherever people and scarce resources interact. Fraud, or even the perception of fraud, can have a serious impact on an organisation's reputation and resources. It can stem from inside or outside the organisation and by its nature is deceitful, dishonest, and often hard to detect. Numerous Corruption and Crime Commission investigations highlight the risks organisations face.

However, there are practical steps organisations can take to reduce fraud risks and build their fraud resistance. These include creation of a strong ethical culture that sets the standard of behaviour for all staff, raising staff awareness of the risks, and implementing good practice controls to manage them.

This audit found that many local governments have not assessed their fraud risks, and do not have comprehensive fraud management plans and programs. Most could do more to educate their staff on integrity polices and controls to reinforce anti-fraud messages and consider fraud risks in their daily duties. Local governments also need to make sure they have clear and easy processes for people to report any fraud concerns.

It was pleasing to find that all the local governments we reviewed had some fraud controls in place and the staff my audit team dealt with during the audit were diligent. But, high staff turnover and work load makes implementing good fraud controls even more of a priority.

I would like to acknowledge the willingness of the entire sector to engage with our questionnaire. Nearly 80% of local governments responded, providing valuable information about fraud approaches across the local government sector.

I encourage all entities to use the principles highlighted in Appendix 2 to build on their existing structures and practices, in a way that best suits their needs.

Executive summary

Introduction

Recent high profile investigations into fraud in the public sector by the Corruption and Crime Commission (CCC) in Western Australia (WA) have featured a number of local government entities (entities).

There are 148 entities in WA. In 2017-18, the sector spent more than $4 billion, employed around 17,000 staff, and administered $45 billion of assets. Fraud in this sector could result in substantial material and reputational losses, and this level of risk calls for entities to implement strong controls and better practice approaches to reduce the threat of fraud.

This audit reviewed whether entities have taken appropriate steps to prevent fraud, through the following lines of inquiry:

1. Have entities implemented a coordinated approach to manage fraud risks?
2. Do entities have adequate controls for preventing and detecting fraud?
3. Do entities respond appropriately to suspected fraud?

The purpose of this audit was to review the systems that entities had in place. We did not seek to identify any specific instances of fraud.

The audit included a sector wide questionnaire on entity approaches to managing fraud risks (see Appendix 3 for a summary of results). We conducted a more detailed review at the:

- Shire of East Pilbara
- Shire of Katanning
- City of Nedlands
- Shire of Serpentine-Jarrahdale
- City of Vincent.

Our sample focussed on entities that had not been part of recent audits, and included entities of varying size, from both metropolitan and regional areas.

Conclusion

Local government entities can do more to prevent fraud. We found entities do have some controls in place, but would benefit from better understanding their specific fraud risks and taking a coordinated approach to managing them.

Our questionnaire found many entities have not assessed their fraud risks, or created a plan to deal with fraud. The responses highlighted gaps in prevention and detection approaches. Many entities can do more to raise staff awareness of fraud, improve their screening processes, and strengthen protections for informants.

Our detailed review of 5 entities confirmed these results. We found they had core integrity policies in place, but none had assessed all their fraud risks, and implemented a coordinated approach to manage them. All entities could build on their current policies and practices to make workplaces more fraud resistant, and improve their reporting avenues to strengthen their ability to respond to fraud.

Background

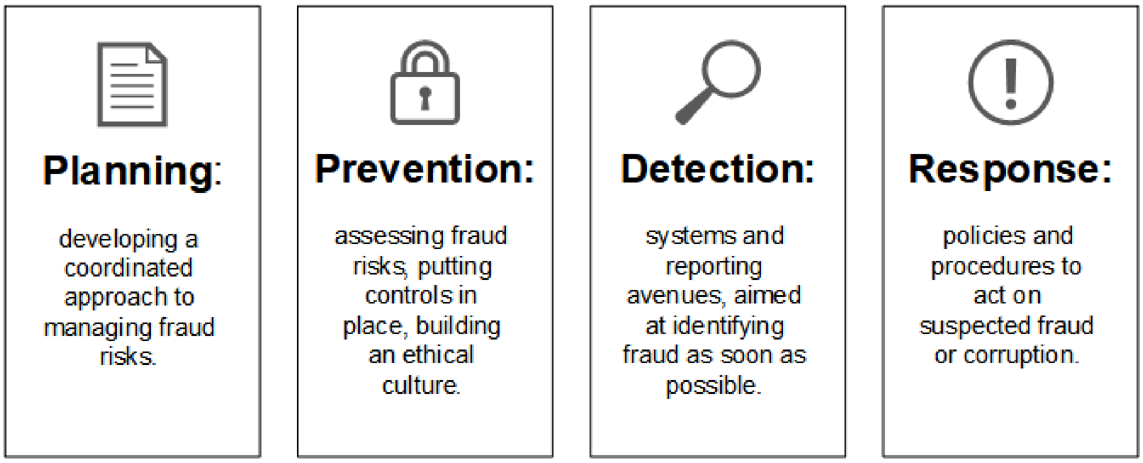
Fraud is the act of obtaining a benefit, financial or otherwise, by deception. By its nature it is deceitful and dishonest, and can be very hard to detect particularly if collusion is involved. It is important that public sector entities design and implement strong internal control frameworks to prevent fraud.

Meeting legislated requirements provides entities with some level of fraud control (Appendix 1), particularly around council decision-making processes. Legislation includes requirements for:

- council and advisors to disclose conflicts of interest
- disclosure of financial interests for some staff
- the creation of Codes of Conduct
- handling of gifts
- when tendering is required for procurement activities.

This is the second report that we have tabled on public sector fraud controls. The previous report in 2013 reviewed 9 state government entities against elements taken from the *Australian Standard AS 8001-2008 Fraud and Corruption Control* (the Standard).

The Standard contains better practice guidance for controlling fraud risks. It is informative, flexible, and forms the basis of approaches in state and local government entities across Australia. It recommends entities tailor an approach that suits their needs, based on 4 components:



Planning: developing a coordinated approach to managing fraud risks.

Prevention: assessing fraud risks, putting controls in place, building an ethical culture.

Detection: systems and reporting avenues, aimed at identifying fraud as soon as possible.

Response: policies and procedures to act on suspected fraud or corruption.

In developing our expectations for entities, we considered:

- key principles from the Standard
- guidance issued to entities by the Department of Local Government, Sport and Cultural Industries
- reports published by the CCC and the Public Sector Commission (PSC)
- guidance material issued by audit offices in other jurisdictions
- the best practice guide for fraud and corruption control published by the Crime and Corruption Commission in Queensland
- international research.

Recommendations

In line with better practice, all entities should ensure they implement a coordinated approach to manage their fraud risks. Entities should:

1. assess fraud risks across their business
2. develop a Fraud and Corruption Control Plan and review it at least once every 2 years
3. develop and implement a periodic fraud awareness training program for all staff
4. ensure that all conflicts of interest are recorded, assessed and appropriate management plans are in place
5. have policies and procedures in place to verify the identity and integrity of employees and suppliers
6. document clear internal processes and systems to report any potential fraud, that include anonymous reporting
7. collect and analyse information received about potential fraud to identify any trends or emerging issues.

Under section 7.12A of the *Local Government Act 1995*, all audited entities are required to prepare an action plan addressing significant matters relevant to their entity for submission to the Minister for Local Government within 3 months of this report being tabled in Parliament and for publication on the entity's website. This action plan should address the points above, to the extent that they are relevant to their entity, as indicated in this report.

Response from audited local government entities

All 5 audited entities supported the audit findings and accepted our recommendations. Appendix 4 includes the full responses from audited entities.

Audit findings

Entities have not implemented a coordinated approach to manage their fraud risks

We found that entities have not developed a good understanding of their fraud risks, or a clear vision of how they will manage them. As a result, entities cannot be sure they have adequate controls in place. These findings are similar to those of our 2013 audit into State government entity fraud controls, which found a lack of risk assessment and planning[1].

Entities have not assessed their business for fraud risks

None of the entities we reviewed had assessed all their fraud risks. We found strategic risk registers included some consideration of external theft and fraud. But, these were incomplete, focussed on external threats, and did not consider all fraud risks. This supports results from our questionnaire, as 25% of respondents told us they had not completed a fraud risk assessment. Completing an assessment would give entities a view of all their risks, and allow them to evaluate their controls.

Twenty-nine of the 116 entities (25%) that responded to this part of our questionnaire advised that they had not assessed their fraud risks. These entities had a combined expenditure of over $310 million in 2017-18.

Entities have not planned how to manage fraud risks

We found that most entities have not developed a Fraud and Corruption Control Plan (Plan). These results are similar to those from our 2013 audit of fraud prevention in State government entities[2]. That audit reviewed 9 State government entities and found none had developed a Plan. Plans are important better practice tools that capture an entity's commitment to manage its fraud risks, communicate its approach, and set timeframes and responsibilities.

Of the entities reviewed, only East Pilbara had developed a Plan. While the Shire completed this in 2013, it has not implemented any of the Plan's actions.

All 5 entities had Codes of Conduct (Codes) and East Pilbara, Nedlands and Vincent also have strategic fraud prevention policies. While these contain anti-fraud information, they are not as comprehensive as a Plan as they do not include controls, or assign timeframes or responsibilities for actions. Without a Plan, entities cannot be sure their approach to managing fraud risks is comprehensive.

Responses to the questionnaire show this is an issue across the sector, as more than half (54%) the entities told us they had not created a Plan.

We received documents from 26 of the entities who told us they had a Plan or equivalent. However, we found only 7 of these contained all the key elements of the Standard[3]. A further 8 contained at least 2 of the elements. Avenues for reporting suspected fraud, key controls to deal with fraud related risks and comprehensive fraud risk assessments were elements that were most commonly absent.

[1] Office of the Auditor General 2013 *Fraud prevention and detection in the Public Sector*. Report 7 – June.

[2] Ibid.

[3] We reviewed the documents for key elements of the Standard including an entity position statement, accountabilities, a fraud risk assessment, outline of key controls, and reporting avenues and protections.

Entities could make themselves more fraud resistant if they strengthen their controls

We found that entities could make their organisations more fraud resistant if they raise staff awareness of risks, improve how they manage conflicts of interests, and better screen employees and suppliers.

Entities need to raise staff awareness of fraud risks

The Standard describes building a strong anti-fraud culture as a key strategy for managing the risk of fraud. Messaging to staff can help entities build and maintain fraud resistant cultures. Entities should commit to a program to raise staff awareness of integrity policies. By tracking participation they can be sure staff are aware of risks, the controls that are in place, and their responsibilities.

We found entities have not established regular programs to raise and maintain staff awareness of fraud risks. None of the entities we reviewed had established a regular training program, or had kept records of staff participation. The questionnaire provided similar results, with 55% of entities advising they did not train staff in fraud risks and controls.

Some of the entities we reviewed have made efforts to raise staff awareness of fraud risks and integrity policies. We found:

- 3 entities had used training, forums, or newsletters to engage staff in managing fraud risks (Figure1)
- 2 entities had tailored the language in their Codes to make them easier for staff to understand. To explain conflicts of interest, Serpentine-Jarrahdale used plain English rather than text from legislation, and Katanning included “real world” examples.

Katanning	Nedlands	Serpentine-Jarrahdale
The Infrastructure Department received refresher training on the Shire’s code of conduct in January 2019.	Information about integrity issues have been included in staff newsletters. For example: • information on ethical decision making – August 2018 • article on conflicts of interest - September 2018.	The Shire has conducted a series of staff forums. For example: • CEO led a forum on fraud controls - March and April 2017 • ‘good governance’ forum - September 2018 • forum on misconduct prevention, including a presentation from the PSC - January 2019.

Source: OAG using entity information

Figure 1. Examples of recent efforts to raise fraud awareness

All the entities we reviewed provided employees with key integrity policies at induction. However, none required staff to revisit the policies. The Standard recommends all employees confirm they understand and follow the Code, and other integrity policies, on a yearly basis. Results from our questionnaire suggest this is an issue across the sector, as 89% of entities told us they do not require staff to do this. Recording annual compliance would give entities a level of assurance that staff are regularly engaging with integrity policies and messages.

Not all conflicts of interest are captured

Three of the entities we reviewed did not capture all the conflicts of interest their staff may face. In line with legislation, entities record conflicts of staff and elected members on matters discussed by council. Entities also document financial, proximity and impartiality interests of elected members and senior staff.

However, processes are not in place to capture, assess and manage any other interests staff have that may conflict with their daily duties. Entities cannot be sure they appropriately manage all conflicts of interest (actual, potential or perceived), as they rely on individual business units to handle operational issues with no formal guidance or process. Staff need to be aware that they have a responsibility to declare any interests that could conflict with performing their public duties. Entities then need to capture and manage those declarations.

Vincent and Serpentine-Jarrahdale have recently implemented processes to better capture all conflicts of interest. Both entities have developed registers to capture the conflict, and require a manager or executive to approve the management plan. During the audit, both entities provided staff with guidance on how and when to make a declaration.

More screening of employees and suppliers would help entities reduce risks

The entities we reviewed did not have adequate policies to screen staff or suppliers. Good screening controls would give entities some assurance of the identity, integrity and credentials of employees and suppliers.

None of the entities we reviewed had policies in place to screen staff. These findings are similar to those in our 2019 audit *Verifying Employee Identities and Credentials*[4].

Despite the lack of policy, 4 entities did retain copies of qualifications and identification. However, none consistently confirmed that qualifications were authentic or checked work histories. One entity did not engage in any police checks or do any checks beyond calling referees. Entities need consistently applied processes to confirm the identity, integrity and academic credentials of potential employees. The Standard also recommends entities screen all new employees and any employee transferring to an executive or high-risk area.

None of the entities we reviewed routinely screened their suppliers. Our questionnaire returned similar results, with less than 30% of respondents conducting media searches, police clearances or verifying directors' details. Purchases over $150,000 are subject to tender which include some checks, including an ABN confirmation and receiving information on the financial position of the supplier. However, smaller purchases are not subject to this process.

To reduce fraud risks, the Standard recommends that entities verify the credentials of suppliers. Entities that have a large number of suppliers should consider a risk-based approach to screening to ensure appropriate use of resources.

Better reporting avenues would help entities detect and respond to fraud

To be well informed, entities need to have strong systems to receive, capture and act on information about potential fraud. International research has shown that organisations most frequently detect fraud through informants (whistleblowers)[5].

[4] Our audit found only 3 of the 8 entities reviewed had policies to verify employee identities and credentials.

[5] Association of Certified Fraud Examiners 2018 *Report to the nations: global study on occupational fraud and abuse*. p4.

We found that it was not always clear how staff, the public or suppliers should report suspected fraud. The entities we reviewed did not have ways for individuals to make anonymous reports of potential fraud, other than Public Interest Disclosures (PID) through the *Public Interest Disclosure Act 2003* (PID Act). They also did not have a process in place to analyse all information they received about potential fraud. Entities may miss important information if reporting avenues are not clear or if reports are not analysed.

Entities need to better communicate how staff, suppliers and the public can report suspicious behaviour

At the entities we reviewed, Codes direct staff to report concerns of fraud to the CEO, deputy, or HR manager. However, there is no guidance for how a staff member would do this. Staff members may be reluctant to go directly to the executive on such a sensitive topic or when the suspicion relates to senior staff. The Standard highlights the need for formalised reporting systems and that these should include multiple avenues. Similarly, the Crime and Corruption Commission in Queensland has advised that employees will feel more confident in making reports if systems are readily accessible and well publicised[6].

The PID Act encourages people to report concerns of wrongdoing in the public sector. Individuals can report concerns to authorised officers or to 1 of the authorities listed in the PID Act (such as the Auditor General for concerns including substantial unauthorised use of public resources). Other external reporting avenues include the CCC, PSC or the Western Australia Police Force.

All the entities we reviewed had clear processes around making a PID and had PID officers in place. However, entities should not rely only on PIDs, as this does not capture all potential reports or allegations. Staff may not wish to engage with the PID process or may not have information suitable for an investigation. The PSC reported that local government entities received 13 PIDs in 2017-18[7].

Our questionnaire showed that many other entities could improve their reporting processes and protections. One third of respondents told us they did not have systems in place to protect staff who reported fraud. Of those that did have protections, 32% told us they relied solely on PIDs. Individuals may be reluctant to report concerns if they do not feel adequately protected.

Entities should include anonymous reporting options to encourage reporting

At the entities we reviewed, internal avenues to report suspected fraud did not include anonymous options. Both the Standard and guidance from other jurisdictions has raised the need for internal reporting to include options for anonymity. Making reports of wrongdoing can be difficult for some people and providing an anonymous option can make it easier.

We note that East Pilbara's Plan directs staff wishing to make an anonymous complaint to external agencies, either the CCC or the PSC. While directing staff to appropriate external reporting options is important, in our view better practice would be for internal reporting to also have anonymous options.

Entities need to better use information they receive about suspected fraud

None of the entities we reviewed have a way to capture, collate and analyse all information about potential fraud. The Standard expects organisations to develop a program and

[6] Queensland Crime and Corruption Commission 2018 *Fraud and Corruption Control: best practice guide* p49.

[7] Public Sector Commission *2018 State of the sector statistical bulletin*: Integrity and Conduct Survey results.

recommends the development of a fraud register. Capturing information in a central location would make it easier for entities to look for trends, identify issues early and act appropriately.

Entities have reported potential fraud to the CCC. The entities we reviewed told us they had reported 4 instances of potential fraud in the past 5 years.

Audit focus and scope

This audit assessed whether local government entities have taken appropriate steps to prevent fraud. We asked the following questions:

1. Have entities implemented a coordinated approach to manage fraud risks?
2. Do entities have adequate controls for preventing and detecting fraud?
3. Do entities respond appropriately to suspected fraud?

During our audit we considered:

- key principles from the Fraud and Corruption Control Standard (AS 8001-2008)
- guidance issued to entities by the Department of Local Government, Sport and Cultural Industries
- guidance material issued by audit offices in other jurisdictions
- reports published by the CCC and the PSC
- the best practice guide for fraud and corruption control published by the Crime and Corruption Commission in Queensland
- international research.

During the audit we:

- provided a questionnaire to all 148 local government entities, requesting information about approaches to managing fraud risks.
    - 118 entities responded to the questionnaire (see Appendix 3)
    - 91 provided copies of their Codes of Conduct
    - 26 provided copies of their Plans. We reviewed the Plans for key elements of the Standard, including an entity position statement, accountabilities, a fraud risk assessment, outline of key controls, and reporting avenues and protections.
- reviewed approaches in more depth at 5 entities. This included interviews with key staff, and reviews of policies, registers and complaints systems. This sample included entities ranging from relatively small to large, from both metropolitan and regional areas.

We did not conduct detailed reviews of procurement, record keeping or systems for verifying employee identities. These areas were the focus of recent performance audits by this Office.

This was a narrow scope performance audit, conducted under section 18 of the *Auditor General Act 2006* and in accordance with Australian Auditing and Assurance Standards. Narrow scope performance audits have a tight focus and generally target entity compliance with legislation, public sector policies and accepted good practice. The approximate cost of undertaking and tabling this audit is $300,000.

Appendix 1: Summary of legislated responsibilities

Entities are required to meet a number of legislated responsibilities that help control fraud risks. A summary of key elements are listed below. This list is not exhaustive.

Legislation	Fraud related requirements
Local Government Act 1995	• disqualifies individuals from becoming elected members due to insolvency, criminal convictions, or misapplication of funds • councils must believe that a person is suitably qualified for the position of CEO, and CEOs must believe that staff are suitably qualified for their positions • all employees must be selected in accordance with the principles of merit and equity • mandates a general need for good government and the creation of a Code of Conduct • council members, the CEO and designated staff members must disclose financial interests' • employees must disclose any interests when they are advising or reporting to council • an audit committee must be formed • sets out penalties for improper use of information
Local Government (Rules of Conduct) Regulations 2007	• requires council members to act ethically, be open and accountable • forbids council members from influencing employees or using their office for personal advantage • council members must declare any interests in matters being discussed at council or audit committee meetings • sets out restrictions on gifts and travel contributions to councillors and requirements for records to be kept
Local Government (Financial Management) Regulations 1996	• CEOs are to establish efficient systems and procedures for collection and custody of money owing to the entity
Local Government (Audit) Regulations 1996	• describes the function of the audit committee • Regulation 17 requires a CEO to review appropriateness and effectiveness of systems and procedures relating to risk management, internal control and legislative compliance. This is then reported to the audit committee
Local Government (Administration) Regulations 1996	• sets out information on disclosure of financial interests • provides detailed information on what value of gifts must be reported and which are prohibited • requires a register of gifts to be publicly accessible • requires Codes of Conduct to contain information on gifts, travel contributions and disclosing interests

Legislation	Fraud related requirements
Local Government (Functions and General) Regulations 1996	• entities must develop a policy for purchases less than, or equal to, $150,000 • purchases worth more than $150,000 must be conducted through tender • sets out requirements for pre-qualified suppliers
Public Interest Disclosure Act 2003	• entities must ○ publish internal procedures for reporting a PID ○ designate at least 1 PID officer to receive reports. They must comply with the Public Sector Commissioner's minimum standards of conduct and integrity

Source: OAG

Appendix 2: Better practice principles

The table below shows key principles on which our audit focused. These principles are not exhaustive. Entities seeking to implement better practice approaches should also consult the Standard, and the guidelines prepared by the Department of Local Government, Sport and Cultural Industries.

Objective	Principle	What we would expect
Planning Develop a coordinated approach to manage fraud risks	Risks are understood	• Fraud risks across organisation are assessed, documented and controls are in place.
	Approach is documented	• Fraud and Corruption Control Plan (Plan) is in place and reviewed at least once every 2 years.
	Internal audit considers fraud risks	• Audit committee engages with internal audit plan to ensure fraud risks are considered.
Prevention Create a fraud resistant organisation	Policy framework is in place	• Integrity policies (such as Codes of Conduct and conflicts of interest) are appropriate, clearly written and available. • Staff regularly engage with integrity policies. For example, signing yearly an understanding of the Code of Conduct. • Fraud prevention and awareness training, newsletters and presentations are used to communicate entities ethical standards to staff.
	Internal controls are in place	• Business processes, especially those assessed as higher risk, have controls that are well documented, updated and understood by all staff. • Entities verify identity and credentials of all new employees and employees transferring to areas of higher risk, including: ○ verify necessary qualifications ○ review of past work history and referee checks ○ criminal background checks ○ confirm professional memberships are valid. • Supplier credentials are checked, particularly for high-risk or high value purchases, including: ○ Confirm ABN ○ confirm directors are not bankrupt or disqualified.

Objective	Principle	What we would expect
Detection Entities are ready to detect fraud	Detection systems are in place	• Entities should implement detection systems, as appropriate to their business needs, to identify potential fraud as soon as possible. • Multiple avenues are in place for staff, the public and suppliers to report concerns. • Reporting processes are well advertised, and include anonymous options.
Response Entities are ready to respond to potential fraud	All information is considered	• Entities should implement processes to record, analyse and escalate all incidents. • Processes are in place to review internal controls after incidents.

Source: OAG

Appendix 3: Summary of local government fraud questionnaire results

Planning

59% are aware of the Standard (118)

54% have not developed a Plan to deal with fraud risks (113)

25% have not assessed their fraud risks (116)

Prevention

100% have a Code of Conduct (112)

15% do not keep a register of all conflicts of interest (112)

28% always conduct supplier background checks (110)

89% do not require staff to engage with the Code yearly (112)

55% do not provide staff with specific training on fraud controls (112)

Detection

90% have mandatory reporting of fraud (110)

32% who have protections for informants, rely solely on PID (68)

34% do not have systems to protect informants (110)

Response

45% do not have a formal process for investigating fraud (110)

61% do not require investigators to be trained (110)

72% do not have a policy to recover losses (110)

89% always, or usually, keep records of fraud (110)

72% always or usually review controls after an incident (110)

Number of responses to question marked in (*)

Source: OAG

Appendix 4: Full responses from audited entities

Shire of East Pilbara

Specific responses to recommendations

The Shire of East Pilbara agreed with all recommendations. They provided additional comments on recommendations:

2. Agree. But it is noted that the Shire of East Pilbara does have a Fraud and Corruption Plan. Our priority should be to deploy the plan effectively within the organisation and to undertake regular reviews internally

4. Agree. Conflicts of interest are recorded for elected members and key officers who are writing reports and/or attending Council meetings. It is noted that conflicts of interest for staff need to be recorded and this practice needs to be embedded further within the organisation.

Shire of Katanning

Specific responses to recommendations

The Shire of Katanning agreed with all recommendations.

City of Nedlands

The City is encouraged by the audit work of the Office of Auditor General in the local government space and believes that its work to date in providing clarity on governance inconsistencies and interpretation in local government, which is long overdue.

Specific responses to recommendations

The City of Nedlands agreed with all recommendations and advised they will aim to implement a streamlined and coordinated approach towards risk management within the next 18 months. They provided additional comment on recommendations:

1. Agree. In the past, the City has conducted an organisation wide Risk Assessment program which incorporated a fraud risk assessment. However, the City will aim to undertake the first full fraud risk assessment within next 18 months.

2. Agree. The City will aim to develop and implement a control plan within 8 months.

3. Agree. 2019/20 training will be scheduled followed by annual training.

4. Agree. The City agrees that all conflicts of interest are to be recorded and assessed. At present, the implemented process is to record, assess and manage the declared conflict of interest by the Elected Members and staff for any matter to be discussed at Council meetings. Based on this recommendation the City agrees that procedures should be in place for assessing and recording all conflicts of interest; however, is not aware of the nature, content or need for management plans to achieve this. The City will aim to implement an appropriate Procedure within 8 months.

5. Agree. It is noted that the need for and extent of verification, is a matter to be considered within proper risk assessment, as part of policy and procedures scope. At present, there are verification processes in place for both employees and suppliers. However, there is definitely room for the improvement in this area. Accordingly, the City will aim to review and update its HR and suppliers' policies and procedures within 12 months.

6. Agree. The City will aim to implement this within 12 months.

7. Agree. Once the work around the implementation of streamlined and coordinated approach towards fraud risk management is completed, the City will be able to perform the above task on an ongoing basis.

Shire of Serpentine-Jarrahdale

The Shire of Serpentine Jarrahdale welcomes the findings and subsequent recommendations of the 2019 Performance Audit for Fraud Prevention in Local Governments. It considers that the report is a balanced representation of areas and a good platform to work towards enhanced fraud management activities.

Specific responses to recommendations

The Shire of Serpentine-Jarrahdale agreed with all recommendations. They provided additional comment on recommendations:

1. Agree. The Shire will continue the fraud risk activities scheduled in the Internal Audit – Interim Audit Plan 2019. Outcomes of the initial risk / control activities will be transitioned to the updated Risk Framework when complete. Timeframe: April 2020.

2. Agree. The Shire will build a framework for management of fraud with a view to integrate into ongoing awareness and training processes inclusive of periodic review. Timeframe: April 2020

3. Agree. The Shire is in the process of implementing a learning and development management system. Induction and code of conduct are scheduled to be the initial modules to be implemented. The modules will be required on a periodic basis and be supported with audit trails and electronic signatures for tracking attendance. Timeframe: December 2019.

4. Agree. Building upon processes implemented to capture all conflicts of interest, the Shire is in the process of rolling out a consistent conflict of interest awareness process and supporting policy / procedure environment. Once the learning and development management system is implemented the Shire will progress to implement a specific module within the system. Timeframe: April 2020.

5. Agree. Employees - Policies will be reviewed to document a risk based approach to the screening of employees including enhancing the approach to assess qualifications, references and background searches. Suppliers - Policies will be reviewed to document a risk based approach to the screening for suppliers including consideration of legal history and checking of supplier Directors. Timeframe: December 2019.

6. Agree. Whistle-blower processes are scheduled to progress. The scope and approach of the processes will be informed by the recommendations of the report. Timeframe: October 2019.

7. Agree. Whistle-blower processes are scheduled to progress. The scope and approach of the processes will be informed by the recommendation of the report. April 2020.

City of Vincent

The City of Vincent (City) accepts the finding in the report and acknowledges that there are gaps in the City's current management and reporting of potential fraud. The City will table the Summary of Findings to its Audit Committee in August 2019, along with a management plan to address the recommendations identified. The management plan will be monitored by the Audit Committee to ensure all items are adequately completed.

Specific responses to recommendations

The City of Vincent agreed with all recommendations. They provided additional comment on recommendations:

1. Governance will develop and implement a program for the annual review of fraud risks across the business. The proposed implementation date is June 2020. The findings of the annual review will be tabled at Audit Committee, with any items requiring action being included in the Audit Log and monitored by the Audit Committee until completion.
2. Governance will review the City's current Fraud and Corruption Prevention Policy and prepare a control plan which incorporates this policy. The proposed implementation date for the plan is June 2020. The plan will be reported to Audit Committee annually and updated as required.
3. Human Resources with the support of Governance will develop and implement an online fraud awareness training program to be completed by all staff. New staff will be required to complete the training as part of their online induction process and current staff will receive notification to complete the training annually via the induction portal. The proposed implementation date is January 2020.
4. The City currently has a register for Elected Members and senior staff as required by the Local Government Act 1995 and a register to capture and manage any other actual, perceived or potential staff conflicts of interest. Governance, in coordination with Human Resources, will ensure all staff are aware of the conflict of interest disclosure requirements and provide training for new staff as part of the induction process.
5. Human Resources will develop and implement a recruitment and selection policy and procedure (which will include identity and integrity checks) for the City. Human Resources will periodically monitor employees for change of circumstances via a declaration form which WALGA are currently preparing to supply to Local Governments. The proposed implementation date is January 2020. Finance will review and update the City's supplier verification process. The proposed implementation date is December 2019.
6. The City will investigate systems and processes to report any potential fraud, including anonymous reporting. The proposed implementation date is December 2020.
7. The fraud reporting system, as referred to in 6. above, should enable this data to be easily compiled. Governance will periodically review the data.

5.2

5.2

5.2

Auditor General’s reports

Report number	2019-20 reports	Date tabled
4	Access to State-Managed Adult Mental Health Services	14 August 2019
3	Delivering Western Australia’s Ambulance Services – Follow-up Audit	31 July 2019
2	Opinion on Ministerial Notification	26 July 2019
1	Opinions on Ministerial Notifications	19 July 2019

5.2

Office of the Auditor General
Serving the Public Interest

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

T: 08 6557 7500
F: 08 6557 7600
E: info@audit.wa.gov.au
W: www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General for
Western Australia

5.3

STANDARDS Australia

AS 8001—2008

Fraud and Corruption Control

Australian STANDARD

AS

This Australian Standard® was prepared by Committee MB-004, Business Governance. It was approved on behalf of the Council of Standards Australia on 26 October 2007.
This Standard was published on 6 March 2008.

The following are represented on Committee MB-004:

- Australian Corporate Lawyers Association
- Australian Federal Police
- Australian Institute of Company Directors
- Australian Institute of Professional Investigators
- Australian Society of Association Executives
- Centre for International Corporate Governance Research, Victoria University
- Chartered Secretaries Australia
- Engineers Australia
- Environment Institute of Australia and New Zeland
- Institute of Internal Auditors – Australia
- IAB Services
- Queensland University of Technology
- Risk Management Institution of Australasia
- Society of Consumer Affairs Professionals
- Transparency International Australia

This Standard was issued in draft form for comment as DR 06651.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

AS 8001—2008

Australian Standard®

Fraud and corruption control

Originated as AS 8001—2003.
Second edition 2008.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 8522 0

5.3

PREFACE

This Standard was prepared by Standards Australia Committee MB-004, Business Governance, to supersede AS 8001—2003.

Major revisions to the Standard include—

- changes to structure and format;
- increased consideration of information systems as an enabler of fraud and corruption and as a means of detecting fraud and corruption;
- expanded guidance on the suggested role of the internal audit function in controlling the risk of fraud and corruption;
- separate consideration of corruption and the ways in which corruption risk can be managed;
- increased emphasis on example setting by senior executives as an important element of an entity's integrity framework;
- upgraded fraud risk assessment methodology (to bring it into line with changes to AS/NZS 4360:2004);
- upgraded employment screening guidelines;
- new customer and supplier vetting guidelines; and
- reference to the role of the external auditor in fraud detection.

The objective of this Standard is to provide an outline for a suggested approach to controlling the risk of fraud and corruption within a wide range of entities across all industry sectors and in government.

This revision reflects recent changes in the approach to controlling fraud and corruption in the Australian economy made necessary by technological advancement and the way business is conducted.

This Standard is part of the Corporate governance series which comprises—

AS 8000	Good governance principles
AS 8001	Fraud and corruption control (this Standard)
AS 8002	Organizational codes of conduct
AS 8003	Corporate social responsibility
AS 8004	Whistleblower protection programs for entities

In addition, the Standard links to other Standards as referred to herein—

AS/NZS 4360	*Risk management* (and companion handbooks—HB 436:2004, *Risk Management Guidelines—Companion to AS/NZS 4360:2004* and HB 158—2006, *Risk management—Delivering assurance based on AS/NZS 4360:2004*)
AS 4811	Employment screening

Additional guidance on applying this Standard in controlling the risk of fraud and corruption can be found in *Fraud Resistance—A practical guide* published by SIRCA and available from Standards Australia.

The term ‘informative’ has been used in this Standard to define the application of the accompanying appendices. An ‘informative’ appendix is for information and guidance only and should not be considered part of the Standard.

CONTENTS

Page

5.3

Page

APPENDICES

INTRODUCTION

Recent events within Australia and internationally suggest a strong nexus between fraud and corruption within entities on the one hand and fundamental governance failure at senior levels on the other.

Many corporate collapses arise from a conflict between the objectives of the entity and the personal objectives of the custodians of the entity's assets—the Directors and senior executives. This has resulted in an increasing incidence of financial reporting manipulation, sometimes excessive payment of remuneration and other benefits for senior executives and, at times, a crisis of confidence within global equity markets.

Managing business risk has, in recent years, increasingly been accepted as an important governance issue. This has been brought into focus by the Corporate Governance Guidelines issued by the Australian Stock Exchange and the CLERP 9 amendments to the *Corporations Act*. By logical extension, controlling the risk of fraud and corruption is a governance issue which must be given due attention by the controllers of all entities. Increasingly, major fraud incidents or endemic corruption within an entity will be viewed as indicative of a failure of the entity's controllers to discharge these more prescribed governance obligations.

Fraud and corruption involving Australian entities

A number of studies and surveys of fraud within the Australian economy have been conducted over the past ten years. The findings of this research[1] suggest:

- Fraud costs the Australian economy at least $3 billion per year.[2]
- The incidence of fraud within the Australian economy is increasing year by year[3] with up to 63% of Australian organizations experiencing economic crime over a two year period.[4]
- The larger the organization the more likely it is that it will suffer fraud or corruption at some point in its business cycle. For example, in one recent survey it was found that one hundred percent of organizations with more than 5000 employees reported at least one incident of economic crime over two years.[5]
- Survey results indicate that Australian organizations may suffer a higher rate of reported fraud than the global average.[6]
- Research into fraud and corruption in Australia over many years has consistently confirmed that, for the majority of Australian business entities (other than those conducting business in banking or insurance sectors), the main source of fraudulent and corrupt conduct will be from within the entity itself—typically for organizations external to the banking and insurance sectors, internal fraud will account for up to 75% in number of incidents and value of loss suffered.[7]

[1] See in particular, PricewaterhouseCoopers, *Global Economic Crime Survey* (Australian results) released in November 2005 and KPMG Australia Fraud Survey released in November 2006.

[2] Australian Institute of Criminology estimate of fraud in the Australian economy (1997).

[3] Statistics maintained by the Australian Institute of Criminology suggest that the rate of fraud reported to Australian police services per 100 000 head of population has doubled on average every ten years since the mid 1950s.

[4] PricewaterhouseCoopers (2005).

[5] PricewaterhouseCoopers (2005).

[6] PricewaterhouseCoopers (2005).

[7] PricewaterhouseCoopers (2005) and KPMG (2006).

- The financial impact of fraud and corruption on the victims, and in particular, Australian entities engaged in some form of business activity, is steadily increasing.
- The average financial loss associated with fraudulent conduct continues to increase.
- The involvement of organized crime in external attack on the financial sector within the Australian economy is increasing. It is apparent also that much external attack on Australian entities is instigated by or at the direction of criminal gangs based in other parts of the world who use tried and tested frauds against Australian entities.
- Identity theft which is made possible by the penetration of information systems within the wider community, the pace of business and increased educational standards of the perpetrators, is becoming the most important fraud-related threat within the Australian economy.
- Many Australian entities are ill-prepared to detect and prevent fraud against their business with many having made little or no progress in developing or implementing any form of effective fraud control strategy.
- A significant and increasing proportion of cases of fraud detected are not reported to the police or other law enforcement agency for investigation.

Fraud examples in Australian business

Examples of fraud (as distinct from the concept of 'corruption' which is dealt with later in this introduction) which occur in Australian business and therefore fall within the intended scope of this Standard are:

- Theft of plant and equipment by employees.[8]
- Theft of inventory by employees.[9]
- False invoicing (involving a staff member of the entity or a person external to the entity creating a fictitious invoice claiming payment for goods or services not delivered or exaggerating the value of goods delivered or services provided).
- Theft of funds other than by way of false invoicing.[10]
- Theft of cash (particularly in retail or other cash businesses) usually involving some form of concealment, e.g. lapping.
- Accounts receivable fraud (misappropriation or misdirection of remittances received by an entity from a debtor).
- Credit card fraud involving the unauthorized use of a credit card or credit card number issued to another person (the most common fraud against the banking sector) or the use of stolen or fraudulently generated credit card numbers by merchants.
- Lending fraud (loan application made in a false name and supported by false documentation).
- Theft of intellectual property or other confidential information.

[8] Theft of plant, equipment, inventory or other property by persons unconnected to the entity suffering the loss and where deception is not involved is not considered 'fraud' for the purposes of this Standard.

[9] Inventory theft is probably the most common employee instigated fraud type within the Australian economy and represents a significant loss in industries that handle large volumes of inventory. In the retail sector for example, it has been estimated by ECR Australia (Efficient Consumer Response) that 1.5% of retail turnover is lost to shrinkage. Traditionally, 45-50% of retail shrinkage is thought to be employee instigated.

[10] Workplace based on-line banking fraud has increased in frequency in recent years. This will typically involve an employee with some form of control over the management of the accounts payable function substituting their own account number for the account number of a legitimate vendor.

- Financial reporting fraud (falsification of the entity's financial statements with a view to obtaining some form of improper financial benefit).
- Release or use of misleading or inaccurate information for the purposes of deceiving, misleading or to hide wrongdoing.
- Insider trading (buying and selling shares on the basis of information coming into the possession of the perpetrator by reason of his or her position but which is not known to investors generally).
- Misuse of position by senior executives or directors in order to gain some form of financial advantage.

Fraudulent conduct by agents of Australian entities

Australian entities themselves (through their Directors and managers as their agents) sometimes become involved as perpetrator of fraudulent conduct in a number of ways including:

- Material and deliberate misstatement of accounting information for an improper purpose (for example to underpin a share price or to meet profitability or cash flow forecasts).
- Overcharging for goods and services in invoices rendered to customers and clients.
- Taking-up as revenue remittances received in error rather than allowing a credit to the payer.
- Tax evasion.
- Money laundering.
- Insider trading.
- Theft of intellectual property.

Explaining the increasing incidence of fraud

The reasons for the increasing incidence of fraud are many and varied but there are a number of consistent and recurring themes:

- The continual striving for greater efficiencies in business which leads to reduced staffing levels and a consequent reduction in internal control adherence.
- The increasing use and reliance on technology and the associated changes in payment systems and channels. Of particular concern is the ease with which commercial crime can operate globally, access accounts in countries on the other side of the globe and then transfer funds very quickly between accounts in a different jurisdiction with the intention of making it impossible to follow the trail let alone recover any of the proceeds.
- The continuing trend towards 'flattening' of organizational structures and the resulting reduction in management focus on enforcing internal controls and managing risk.
- Rapid and continuous changes to business operations.
- The increasing pace of business.
- The inability of the criminal justice system, the police, the Australian Securities and Investments Commission and other law enforcement agencies and the Courts, to keep pace with the ever-increasing workload and greater complexity of matters reported.
- The accessibility of gambling which has become a significant motivator for employees to commit fraud against their employer.
- Greater complexity of business relationships.

- Changing remuneration and incentive structures and arrangements.

The value to an entity of information held cannot be overstated. The loss of information through unauthorized system access can cause significant damage to an entity's reputation in the short- and long-term and must be treated as a serious threat. Controlling the risk of information theft by unauthorized internal or external access should be a matter of priority for entities whose businesses rely heavily on the information held.

Corruption involving Australian entities

Transparency International's *Corruption Perception Index* ('CPI') is a measure of the perception of the propensity for corruption of public officials within each country surveyed. The 2007 survey of 179 countries[11] found that Australia ranked equal 11th in terms of transparency in business dealings within the country. In other words, the Australian economy was seen as having a relatively low propensity for payment of bribes to the country's public officials in their business dealings with the private sector.

This compares with the *Bribe Payers Index 2006*[12] ('BPI') where Australia was ranked third out of the world's 30 leading exporting countries in terms of its perceived transparency in business dealings with public officials in foreign economies. This means that Australia is perceived as having a relatively low likelihood of paying bribes to public officials in foreign jurisdictions.

While this might be seen as a relatively good result for Australia, it does underscore the fact that there is at least the perception if not the reality of a measurable level of public corruption within the Australian economy.

Corrupt conduct to which Australian entities are subject and which are therefore within the intended scope of a corruption control program contemplated by this Standard include:

- Payment or receipt of secret commissions (bribes), which may be paid in money or in some other form of value to the receiver (e.g. building projects completed at an employee's private residence) and may relate to a specific decision or action by the receiver or generally.
- Release of confidential information for other than a proper business purpose in exchange for some form of non-financial benefit or advantage accruing to the employee releasing the information.
- Collusive tendering (the act of multiple tenderers for a particular contract colluding in preparation of their bids).
- Payment or solicitation of donations for an improper political purpose.
- Serious conflict of interest involving a Director or senior executive of an entity or other entity acting in his or her own self-interest rather than the interests of the entity to which he or she has been appointed (e.g. failing to declare to a Board an interest in a transaction the entity is about to enter into or excessive payment of remuneration to Directors and senior executives).
- Serious nepotism and cronyism where the appointee is inadequately qualified to perform the role to which he or she has been appointed.

[11] Transparency International *Corruption Perception Index* 2007 http://www.transparency.org/policy_research/surveys_indices/cpi/2007/ 'The index defines corruption as the abuse of public office for private gain, and measures the degree to which corruption is perceived to exist among a country's public officials and politicians'.

[12] Transparency International *Bribe Payers Index* 2006

- Manipulation of the procurement process by favouring one tenderer over others or selectively providing information to some tenderers. This frequently involves allowing tenderers to resubmit a 'non-complying' tender after being provided with the details of other bids.
- Gifts or entertainment intended to achieve a specific or generic commercial outcome in the short- or long-term—an essential element rendering conduct of this type corrupt would be that it is in breach of the entity's values, behavioural code or gifts policy (or that of any relevant external party's values or behavioural code) or that it was done without the appropriate transparency within one or more of the entities affected.
- Bribing officials (locally or in foreign jurisdictions) in order to secure a contract for the supply of goods or services.
- Private sector to private sector secret commissions to secure contracts.

Losses associated with the corruption of the procurement process result from reduced competition and the acceptance of substandard delivery of goods and services that would normally be rejected.

Private and public sector entities may also suffer loss if the winning tenderer attempts to recover the cost of the secret commission paid by loading the value of the bid either before or after the contract is awarded.

Managing the risks

An entity's approach to managing the risks of fraud and corruption should be underpinned by an organization-wide policy developed with internal and external consultation with appropriate benchmarking against established best practice prevention and detection programs and standards. It should apply the principles of sound risk management, planning, monitoring and remedial action.

This Standard aims to provide entities with the tools they need to apply these general risk management principles to the control of fraud and corruption. While the Standard aims to provide a high-level framework for organizations to use in developing an anti-fraud program, additional guidance can be found in *Fraud Resistance—A practical guide* (SIRCA, 2003).

STANDARDS AUSTRALIA

Australian Standard
Fraud and corruption control

SECTION 1 SCOPE AND GENERAL

1.1 SCOPE

This Standard provides an outline for an approach to controlling fraud and corruption and, subject to the guidance at Clause 1.2 below, is intended to apply to all entities including government sector agencies, publicly listed corporations, private corporations, other business entities and not-for-profit organizations engaged in business or business-like activities.

Fraud and corruption contemplated by the Standard fall into three main categories[13]—

(a) fraud involving the misappropriation of assets;

(b) fraud involving the manipulation of financial reporting (either internal or external to the reporting entity); and

(c) corruption involving abuse of position for personal gain.

1.2 APPLICATION

While this Standard is intended to apply to all entities operating in Australia, the extent to which it would be applicable to individual entities will be dependent on the entity's—

(a) size;

(b) turnover;

(c) business diversity;

(d) geographic spread;

(e) reliance on technology; and

(f) the industry in which it operates.

By way of general guidance, it is anticipated that the whole Standard would apply to publicly listed corporations, large privately owned corporations and all government departments and agencies. These entities should typically look to implement this Standard in its entirety for maximum effect or to ensure that pre-existing fraud and corruption control measures are at least as robust as in this Standard.

Only relevant parts of this Standard are applicable to small and medium sized enterprises.

[13] Refer to Clause 1.7.3. for a definition of 'corruption' and to Clause 1.7.8 for a definition of 'fraud'.

1.3 MINIMUM ACCEPTABLE COMPLIANCE AND GUIDANCE PROVISIONS

Throughout this document, text given in bold is intended to represent minimum acceptable compliance for entities seeking to fully comply with the Standard. Content given in plain text is provided as guidance in interpreting and implementing the minimum acceptable compliance elements given in bold. Any entity claiming to be fully compliant with the Standard will, as a minimum, have implemented all of the minimum acceptable compliance level elements set out herein.

1.4 OBJECTIVE

The objective of this Standard is to outline a suggested approach to controlling fraud and corruption against and by Australian entities.[14]

The distinction between fraudulent and corrupt conduct against or by Australian entities is an important one because they involve quite different considerations and the differentiation is not just a matter of internal and external environments. In the first category, the entity is the victim or intended victim and will suffer, in most cases, a relatively minor impact to its reputation (depending on the quantum) should a fraud or corruption incident occur in addition to any economic loss suffered.

In the second category, the entity will usually be a beneficiary of the conduct until the conduct is discovered and exposed in which case the reputational impact on the organization and its business is likely to be substantial. Apart from the need to demonstrate that an entity is a responsible corporate citizen, avoidance of fraudulent or corrupt conduct by or on behalf of Australian entities is essential in order to safeguard the entity's ongoing reputation, which, once damaged, may prove difficult to repair.

The Standard is intended to be practical and effective guidance for entities wishing to implement a fraud and corruption control program covering the risks of fraud and corruption committed within the entity (with the entity as victim) as well as fraud and corruption committed by or in the name of the entity.

The Standard proposes an approach to controlling fraud and corruption through a process of—

(a) establishing the entity's fraud and corruption control objectives and values;

(b) setting the entity's anti-fraud and anti-corruption policies;

(c) developing, implementing, promulgating and maintaining an holistic integrity framework;

(d) fraud and corruption control planning;

(e) risk management including all aspects of identification, analysis, evaluation treatment, implementation, communication, monitoring and reporting;

(f) implementation of treatment strategies for fraud and corruption risks with a particular focus on intolerable risk;

(g) ongoing monitoring and improvement;

(h) awareness training;

(i) establishing clear accountability structures in terms of response and escalation of the investigation;

(j) establishing clear reporting policies and procedures;

(k) setting guidelines for the recovery of the proceeds of fraud or corruption; and

[14] Where the entity is the victim of fraud or corruption on the one hand and the perpetrator of fraud or corruption on the other.

(l) implementing other relevant strategies.[15]

Adoption of this Standard requires an appropriate level of forward planning and application of a structured risk management approach. The application of contemporary risk management principles is seen as fundamental to the prevention of fraud and corruption.

The objective of the fraud and corruption control program outlined by this Standard is the —

(i) elimination of internally and externally instigated fraud and corruption against the entity;

(ii) timely detection of all instances of fraud and corruption against the entity in the event that preventative strategies fail;

(iii) recovery for the entity of all property dishonestly appropriated or secure compensation equivalent to any loss suffered as a result of fraudulent or corrupt conduct; and

(iv) suppression of fraud and corruption by entities against other entities.[16]

While 'elimination' of fraud and corruption will, for many entities, be unachievable, it nevertheless should remain the ultimate objective of a fraud and corruption risk mitigation program subject to the appropriate cost-benefit analysis.

In some Australian industry sectors, there is an argument that fraud and corruption is so entrenched that it can never be fully eradicated. For example, it is unfeasible for externally instigated fraud to be eliminated within the banking sector—the nature of banking is such that a certain level of fraud and attempted fraud will always exist. On the other hand, in many entities operating within certain industry sectors, the complete elimination of opportunistic 'one-off' fraud and corruption incidents by application of an effective risk management approach would be feasible.

Any fraud prevention program will need to have regard to the resourcing constraints of the entity and the realities of the industry in which it operates.

1.5 REFERENCED DOCUMENTS

This Standard should be read, construed and applied in conjunction with the following Standards and Handbooks:

AS	
4811—2006	Employment screening
8000—2003	Good governance principles
8002—2003	Organizational codes of conduct
8003—2003	Corporate social responsibility
8004—2003	Whistleblower protection systems for entities
AS/NZS	
4360:2004	Risk management
HB	
158—2006	Delivering assurance based on AS/NZS 4360:2004 Risk Management
436:2004	Risk Management Guidelines (Companion to AS/NZS 4360:2004)

[15] Derived in part from the *Commonwealth Fraud Control Guidelines*.

[16] For example, corrupt activity by an entity involving the payment of bribes to officials in a foreign jurisdiction as defined within the *Criminal Code Act 1995 (Cwth)*.

5.3

AS 8001-2008 Fraud and corruption control